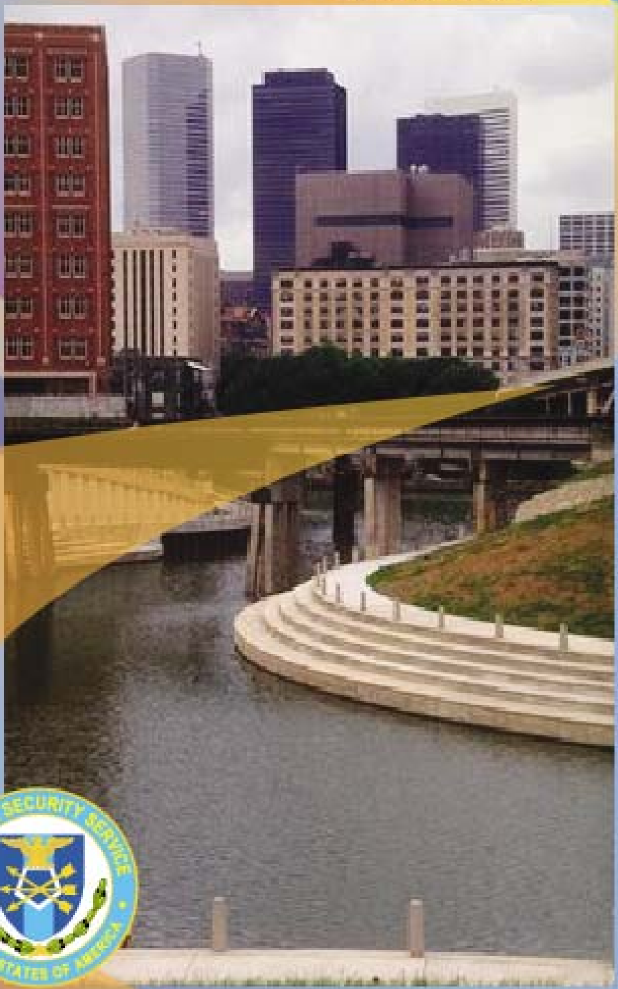
Self Inspection Handbook for NISP Contractors

October 2004



DSSACADEMY
Defense Security Service Academy

Security through Knowledge

Self-Inspection Handbook for NISP Contractors
TABLE OF CONTENTS

ELEMENTS OF INSPECTION

INSPECTION ADDENDUM

SELF-INSPECTION HANDBOOK FOR NISP CONTRACTORS

The Contractor Security Review Requirement

> "Contractors shall review their security system on a continuing basis and shall conduct a formal self-inspection at intervals consistent with risk management principles." **[1-207b, NISPOM]**

The Contractor Self-Inspection Handbook

The National Industrial Security Program Operating Manual (NISPOM) requires all participants in the National Industrial Security Program (NISP) to conduct their own security reviews (self-inspections). This Self-Inspection Handbook contains the NISPOM's main requirements in check list form. The requirements are arranged into "Elements of Inspection." This handbook also suggests various techniques to enhance the quality of your inspection.

The Self-Inspection check list is a list of the more prominent NISPOM security requirements in question form. The basis of each question is found in the NISPOM paragraph cited. You may discover the answer to each question by examining your facility's security program. Your immediate task is to determine which of these requirements relates to your security program. These questions are located within alphabetical delineated areas (A thru X), of common security concern. Traditionally known as the ***"Elements of Inspection,"*** they combine to make up your Self-Inspection check list.

The first three Elements of Inspection: (A) <u>Facility Security Clearance (FCL)</u>, (B) <u>Access Authorizations</u>, and (C) <u>Security</u> <u>Education</u> must be covered during the inspection of all cleared facilities. Any remaining elements need only be covered if they relate to your security program. If you have a question about the relevancy of any element in this self inspection guide for your facility, please contact your IS Respresentative for guidance. A look at your Standard Practice Procedure (SPP), (if you have one) will also provide clues. Of course, as your program becomes more involved with classified information (e.g., changing from a non-possessing to a possessing facility), you will have to expand your review process to include those new elements of inspection. Remember also that <u>not all</u> of the questions (requirements) within each relevant area relate to your program. The best way to determine this is to review each question (requirement) in the context of your industrial security program. If your involvement with classified information invokes the requirement, your procedures should comply with it. Reading each question in the relevant areas of inspection is a means to become knowledgeable of the NISPOM requirements. This handbook is presented as a job aid to assist in conducting required self inspections. In all cases the regulatory guidance takes priority over company established procedures.

Inspection Techniques

To get a clear picture of the state of security at your facility you must (1) know the requirements by which you are inspected, (this is where the check list will help), (2) know your facility's physical layout (i.e., where the classified is stored, worked on, etc.), and (3) have knowledge of the processes involved in the classified programs at your facility. Remember, your primary sources of information are ***documents*** and ***people***.

Your job as the FSO is to *verify* and *validate* that your facility security program is properly protecting classified material and information. To do this, simply review the self-inspection questions against appropriate documentation, people and their actions, and classified information involved in the facility's industrial security program. This is where the self-inspection check list comes in handy. It not only gives you the manual's requirements, but it organizes them into elements of common security concern. These elements should not be held mutually exclusive during the inspection process. In fact, it will become obvious to you that they frequently interrelate.

Interview Techniques

A quality self-inspection depends on your ability to ask questions which may identify security problems. Seek information about *current* procedures, and *change*s which could affect future actions. Get out of your office and into the facility working environment. Talk to the people!

□ All questions should be considered in the present and future sense.

□ Let people tell their story. Ask open ended questions.

□ Let people show you how they perform their job while handling classified information.

□ Follow-up the check list questions with your own questions.

□ Keep good notes for future reference and corrective action.

The Self-Inspection Check List

A. FACILITY CLEARANCE				
NISPOM REF:	**Question:**	**YES**	**NO**	**N/A**
2-111	Are the DD Forms 441 and/or 441-1, SF 328, and DD Form 381-R, available, properly executed and maintained in current status?			
1-302h	Have all changes affecting the condition of the FCL been reported to the DSS Field Office?			
2-108	Does the home office have an FCL at the same or higher level than any cleared facility within the Multiple Facility Organization?			
2-104	Are the senior management official, the FSO, and other Key Management Personnel cleared as required in connection with the FCL?			
2-106a-b	Have the proper exclusion procedures been conducted for uncleared company officials?			
1-302d	Have the required reports been submitted to DISCO regarding employee Representatives of a Foreign Interest?			

B. ACCESS AUTHORIZATIONS				
NISPOM REF:	**Question:**	**YES**	**NO**	**N/A**
	Has all the information in JPAS / JCAVS related ot this facility's employees been validated?			
	Does each employee's JCAVS record indicate an appropriate "eligibility" and "access?"			
	Have all JCAVS users and account managers been officially appointed, issued unique user names and passwords and given the appropriate level in the JPAS / JCAVS?			
	Have all JCAVS users received training appropriate for their duties and responsibilities?			
2-219	Is a current record maintained of all cleared employees at each facility?			
2-200d	Are the number of clearances held to a minimum consistent with contractual requirements?			
2-204	Are all pre-employment clearance applications (if any) based on a written offer and acceptance of employment?			
Chap. 2, Sec 2	Are all required forms and information, regarding cleared personnel, furnished to DISCO?			
2-218	Are employees in process for security clearances informed of their options regarding completion of the privacy portions of the SF 86 application form?			
2-218	Are procedures in place to ensure that the applicant's SF 86 and fingerprint cards are authentic, legible and complete to avoid clearance-processing delays?			
1-302	Does the contractor provide reports on all cleared employees to the DISCO or the DSS Field Office as required?			

C. SECURITY EDUCATION

NISPOM REF:	Question:	YES	NO	N/A
1-206, 3-100 - 3-108	Are all cleared employees provided with security training and briefings commensurate with their involvement with classified information?			
3-104	Do cleared persons at other locations receive the required security training?			
3-105	Are SF 312's properly executed by cleared employees prior to accessing classified and forwarded to DISCO for retention?			
3-105	Are refusals to execute the SF 312 reported to DISCO?			
3-106	Do initial security briefings contain the minimum required information?			
3-107	Does the security education program include refresher security briefings?			

Conduct personnel interviews in the work place during inspection tours of the facility and determine the effectiveness of your security education program. What do the employees remember from the last security briefing? Have them demonstrate the application of security procedures in their job function.

3-108	Are cleared employees debriefed at the time of a PCL's termination, suspension, revocation, or Facility (security) Clearance (FCL) termination?			
1-300	Are there established internal procedures that ensure cleared employees' awareness of their responsibilities for reporting pertinent information to the FSO, the FBI, and other Federal authorities as required by the NISPOM?			
1-301 - 1-302	Is there an effective procedure for submission of required reports to the FBI, the DSS, and DISCO?			
3-103, 9-202	Are Government special security briefings and debriefings provided by the DSS or GCA when required?			
1-304	Is there a graduated scale of administrative disciplinary action in the event of violations or negligence?			
1-208	Are employees aware of the Defense Hotline?			

The Defense Hotline
The Pentagon
Washington, D.C. 20301-1900

(800) 424-9098
(703) 604-8569

1-204	Does management support the industrial security program?			

D. STANDARD PRACTICE PROCEDURES (SPP)

NISPOM REF:	Question:	YES	NO	N/A
1-202	Is the SPP current and does it adequately implement the requirements of the NISPOM?			

Remember that a written SPP must be prepared when the FSO or the IS Representative believes it necessary for the proper safeguarding of classified. [1-202]

E. SUBCONTRACTING

NISPOM REF:	Question:	YES	NO	N/A
7-101	Are all required actions completed prior to release or disclosure of classified information to sub-contractors?			
7-102	Are the clearance status and safeguarding capability of all subcontractors determined as required?			
7-102c	Do requests for facility clearance or safeguarding include the required information?			
7-102d	Are all requests for facility clearance of prospective contractors based on bona fide procurement needs?			
7-102d	Is sufficient lead time allowed between the award of a classified subcontract and the facility clearance process time for an uncleared bidder?			
7-103	In the case of a prime contractor, is adequate security classification guidance incorporated into each classified subcontract?			
7-103	Are contractor-prepared *Contract Security Classification Specifications* (DD 254) signed by a designated contractor official?			
7-103a	Are original *Contract Security Classification Specifications* (DD 254) included with classified solicitations?			
7-103b	Are revised *Contract Security Classification Specifications* (DD 254) issued as necessary?			
7-105	In the case of a prime contractor, is approval obtained from the Government Contracting Activity for subcontractor retention of classified information associated with a completed contract?			

F. VISIT CONTROL

NISPOM REF:	Question:	YES	NO	N/A
	Are visit authorization requests sent and received through JCAVS whenever possible?			
6-101	Do all classified visits require access to or disclosure of classified information?			
6-101	Does the notification of classified visits allow sufficient lead time for the receiver's timely approval?			
6-103 **6-104**	Do Visit Authorization ***r***equests include the required information, and are they updated to reflect changes in the status of that information?			
6-105	Are procedures established to ensure positive identification of visitors prior to disclosure of classified?			
6-106	Are procedures established to ensure that visitors are only afforded access to classified information consistent with their visit (i.e., need-to-know)?			
6-107	Does the facility Visitor Record include the required information?			
6-108	Are long-term visitors governed by the security procedures of the host contractor?			
6-109b	Has the approval of the relevant Government Contracting Activity (GCA) been obtained prior to the disclosure of classified material during non-contract related visits?			

G. CLASSIFICATION

NISPOM REF:	Question:	YES	NO	N/A
4-103	Is all classification guidance adequate and is the *Contract Security Classification Specification* provided as required?			
4-103b	Does the Government Contracting Activity issue revised *Contract Security Classification Specifications* (DD Form 254) as needed?			
4-102	Are there adequate procedures for applying derivative classification to classified material being created, extracted, or summarized?			
4-104	Is improper or inadequate classification guidance being challenged?			
4-103c	Upon completion of a classified contract, did proper disposal of the relevant classified information take place?			
4-105	Is contractor-developed information appropriately classified, marked, and protected?			
4-107	Are downgrading and declassification actions accomplished as required, and is action taken to update records when changing the classification markings?			

H. EMPLOYEE IDENTIFICATION

NISPOM REF:	Question:	YES	NO	N/A
5-410b	Do personnel possess the required identification card or badge when employed as Couriers, Handcarriers or Escorts?			
5-313b	Do ID cards or badges, used in conjunction with Automated Access Control Systems, meet NISPOM standards?			

Security procedures should maximize the use of personal recognition verification for access to classified material. Note that the NISPOM makes only passing reference to IDs and badges for use in specific instances. When such programs are employed as part of your security-in-depth procedures, the specifics should be reviewed with your IS representative.

I. FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE				
NISPOM REF:	**Question:**	**YES**	**NO**	**N/A**
	The following questions apply to all contractors.			
2-301b, 2-302	Is the contractor under any Foreign Ownership, Control, or Influence (FOCI) which could adversely affect performance on classified contracts?			
2-302	Has the contractor reported the presence of any/all FOCI factors to the DSS Field Office in the manner prescribed?			
2-302b	Does the SF 328 “Certificate Pertaining to Foreign Interests” contain current and accurate information? Has the most current information related to the SF 328 been provided to the DSS Field Office?			
2-302b	Has the contractor executed an SF 328 every 5 years regardless of whether **any** changes have occurred?			
2-303b	Has the DSS Field Office been notified of negotiations for merger, acquisition, or takeover by a foreign person?			
	The following questions apply to facilities involved with FOCI.			
2-305	Has a FOCI Negation Plan been submitted to the DSS Field Office?			
2-307	Do contractor senior management officials of companies, operating under a Voting Trust, Proxy Agreement, Special Security Agreement or Security Control Agreement, meet annually with the DSS to review the effectiveness of the arrangement?			
2-307b	Is an annual Implementation and Compliance Report submitted to the DSS Field Office?			
2-308	Has a Government Security Committee been appointed from the Board of Directors under a Voting Trust, Proxy Agreement, Special Security Agreement (SSA), or Security Control Agreement (SCA)?			
2-309	Have companies cleared under a Special Security Agreement received the special authorization needed to access **"proscribed information?”** Proscribed information is TOP SECRET/Restricted Data/Communications Security/Special Access Programs and Sensitive Compartmented Information. The special authorization must be manifested by a favorable national interest determination that must be program/project/contract specific.			
2-310	Has the contractor developed a Technology Control Plan (TCP), approved by the DSS, when cleared under a Voting Trust, Proxy Agreement, SSA, or SCA?			

J. PUBLIC RELEASE				
NISPOM REF:	**Question:**	**YES**	**NO**	**N/A**
5-511	Was approval of the Government Contracting Activity obtained prior to public disclosure of information pertaining to a classified contract?			
5-511a	Is a copy of each approved "request for release" retained for one inspection cycle for review by the DSS Field Office?			

K. CLASSIFIED STORAGE				
NISPOM REF:	**Question:**	**YES**	**NO**	**N/A**
5-102a	Is there a system of security checks at the close of each working day to ensure that classified material is secured?			
5-103	Is a system of perimeter controls maintained to deter or detect unauthorized introduction or removal of classified from the facility?			
5-104	Are procedures developed for the safeguarding of classified material during an emergency?			
5-302	Is TOP SECRET classified stored only in approved GSA security containers, approved vaults, or Closed Areas with supplemental protection?			
5-303	If SECRET material is stored in containers as described in 5-503, is supplemental protection being used during non-working hours?			
5-303 **5-307**	Is supplemental protection provided for all SECRET classified not stored in GSA containers, approved vaults, or Closed Areas?			
5-306	Are Closed Areas constructed in accordance with the requirements of the NISPOM?			
5-306a	Has DSS approval been granted for the open storage of documents in Closed Areas?			
5-308	Is the number of people possessing knowledge of the combinations to security containers minimized?			
5-308a	Is a record of the names of people having knowledge of the combinations to security containers maintained?			
5-308b	Are security containers, vaults, cabinets, and other authorized storage containers kept locked when not under direct supervision of an authorized person?			
5-308c-d	When combinations to classified containers are placed in written form, are they marked and stored as required?			
5-309	Are combinations to security containers changed by authorized persons when required?			
5-311	Are General Services Administration-approved containers repaired as required by the NISPOM?			

If Supplanting Access Control Systems are used, do they meet NISPOM criteria, 5-313 & 5-314, and are they approved by the FSO? (5-312)

	Intrusion Detection System Concerns			
NISPOM REF:	**Question:**	**YES**	**NO**	**N/A**
5-307 **5-900**	Do intrusion detection systems (IDS), utilized as supplemental protection, meet NISPOM requirements?			

Remember that GSA security containers and approved vaults secured with a locking device meeting Fed. Spec. FF-L-2740 may waive the supplemental protection requirement. [see 5-307c].

When guards are authorized as supplemental protection [see 5-307b], required patrol is two hours for TOP SECRET and four hours for SECRET.

5-900 **5-901**	Are Intrusion Detection Systems (IDS) approved by DSS prior to installation as supplemental protection?			
5-902	Are trained alarm monitors cleared to the SECRET level and in continuous attendance when the IDS is in operation?			
5-902	Are alarms activated immediately at the end of business?			
5-902d-e	Are alarm records maintained as required?			
5-903a (3)	Does the Central Alarm Station report “Failure to Respond to Alarm” incidents to the DSS as required?			

Commercial Central Station Alarm Company guards do not require clearance unless their duties afford them the opportunity to access classified material when responding to alarms. [5-903a(2)]

5-904 **5-905**	Are all IDS at the contractor facility installed by UL-listed installers and so certified?			

L. MARKINGS				
NISPOM REF:	**Question:**	**YES**	**NO**	**N/A**
4-200 **4-201**	Is all classified material, regardless of its physical form, marked properly?			
4-202	Is all classified material marked to show the name and address of the facility responsible for its preparation and the date of preparation?			
4-203	Are overall markings marked conspicuously as required?			
4-206	Are portions of classified documents properly marked?			
4-202 - 4-208	Are all additional markings applied to classified as required?			
4-210	Are special types of classified material marked as required?			
4-213	Are classification markings applied to unclassified compilations as required?			
4-216	Are downgrading/declassification notations properly completed?			

Holders of classified material may take automatic downgrading or declassification action as specified without further authority. [4-216a]

4-218	Does the contractor follow NISPOM procedure when classified material is distributed without proper classification or when it is upgraded?			

M. TRANSMISSION

NISPOM REF:	Question:	YES	NO	N/A
5-401	Is classified information properly prepared for transmission outside the facility?			
5-401	Are receipts included when classified transmission requires?			
5-401	Is a suspense system established to track transmitted documents until the signed receipt is returned?			
5-202 **5-204** **5-401**	Are procedures established for proper receipt and inspection of classified transmittals and are returned receipts retained for two years?			
5-402 **5-403** **5-404**	Are authorized methods used to transmit classified outside the facility?			

Remember that transmission of TOP SECRET, outside the facility requires written authorization from the Government Contracting Authority. [5-402]

2-100	Is the facility clearance and safeguarding capability of the receiving facility determined prior to transmission of classified?			
5-410	Are Couriers, Handcarriers, and Escorts properly briefed?			
5-410	Is handcarrying of classified material outside the facility properly authorized, inventoried, and safeguarded during transmission?			
5-411	Is handcarrying aboard commercial aircraft accomplished in accordance with required procedures?			
5-408 **5-409**	Are classified shipments made only in accordance with the NISPOM or instructions from the contracting authority?			
5-408	Does the contractor use a qualified carrier, authorized by the Government, when shipping classified material?			
5-412 **5-413**	Are sufficient numbers of escorts assigned to classified shipments and are they briefed on their responsibilities?			

For information concerning international transfer of classified, see International Operations [Chap. 10, Sec. 4, NISPOM].

N. CLASSIFIED MATERIAL CONTROLS

NISPOM REF:	Question:	YES	NO	N/A
5-100	Do contractor employees understand their safeguarding responsibilities?			

Facility walk-throughs are a good way to determine employee knowledge of safeguarding classified when in-use. Interview and observe how classified is handled in the work place.

5-201	Is the contractor's information management system capable of facilitating the retrieval and disposition of classified material as required?			

Test your system for document retrieval by conducting forward and reverse checks of your classified holdings. Take a sample of classified material from your information management register and attempt to locate it within your facility. Conversely, conduct spot checks at sample locations throughout the facility where classified is stored. Identify items and determine if they are reconciled in the information management system.

5-202	Are external receipt and dispatch records maintained as required?			
5-203	Are TOP SECRET control officials designated at facilities possessing TOP SECRET classified?			
5-203	Are TOP SECRET accountability records maintained as required and is an annual inventory conducted?			
5-204	Is all classified material received at the contractor facility and delivered directly to designated personnel?			
5-205	Are contractor-generated TOP SECRET documents and “working papers” entered into accountability as required?			

Remember that all classified working papers must be marked with (1) the “working paper” designation, (2) the overall classification level, and (3) the date of creation. However, accountability requirements relate only to TOP SECRET.

5-103	Does the contractor maintain a system of controls to deter or detect unauthorized introduction or removal of classified from the facility?			
1-300 **1-303**	Do contractor employees promptly report the loss, compromise, or suspected compromise of classified to the FSO?			
5-104	Are procedures adequate to protect classified during emergencies?			
5-102	Are security checks conducted at the end of each working day to ensure proper storage of classified materials?			

Conduct a walk-through inspection during lunch breaks, after hours, and on late work shifts, if classified is being accessed, to determine the actual state of security at your facility. [1-207b].

O. CONTROLLED ACCESS AREAS

NISPOM REF:	Question:	YES	NO	N/A
5-305	Do Restricted Areas have clearly defined perimeters and is all classified material properly secured when the area is unattended?			
5-306 **5-308**	Are Closed Areas approved by the DSS and properly constructed in accordance with the NISPOM?			

Remember that Closed Areas require DSS Field Office approval and an approved Intrusion Detection System (IDS) unless security guards were approved prior to 1995. When guards are authorized as supplemental protection (see 5-307b), the required patrol is two hours for TOP SECRET and four hours for SECRET.

5-302 **5-303** **5-306** **5-307**	Are Closed Areas storing SECRET or TOP SECRET material afforded adequate supplemental protection during non-working hours?			

Supplemental Controls are not required for SECRET classified storage during non-working hours. (If Security In-Depth has been approved.) See definition of Working Hours, Apx. C, NISPOM.

5-312 - **5-314**	Do supplanting access control devices used for Closed Area access control, during working hours, meet NISPOM requirements and have FSO approval prior to installation?			

Watch entrances to Closed Areas to determine the procedure employed when supplanting access control devices are utilized. Are authorized users allowing unauthorized persons to piggy-back into the area?

5-306	Are persons without the proper clearance and need-to-know escorted at all times when in a Closed Area?			

Intrusion Detection System Concerns

NISPOM REF:	Question:	YES	NO	N/A
Chap. 5, Sec. 9 **5-900** **5-901**	Is IDS approved by DSS prior to installation as supplemental protection and does it meet NISPOM or UL 2050 standards as required?			
5-902	Are trained alarm monitors cleared to the SECRET level in continuous attendance when the IDS is in operation?			
5-902	Are alarms activated at the end of business?			
5-902d-e	Are alarm records maintained as required?			
5-903a (3)	Does the Central Alarm Station report failure to respond to alarm incidents to the CSA as required?			

Commercial Central Station Alarm Company guards do not require a personnel clearance unless their duties afford them the opportunity to access classified material when responding to those alarms. [5-903a(2)]

5-904 **5-905**	Has a UL 2050 CRZH certificate been issued?			

P. DISPOSITION

NISPOM REF:	Question:	YES	NO	N/A
5-700b	Is a program established to review classified holdings on a recurring basis for the purpose of reduction?			
5-701	Is the disposition of classified material accomplished in accordance with the required schedule?			
5-702	Is retention authority requested as required?			
5-704	Is classified material destroyed as soon as possible after it has served its purpose?			
5-705	Is an effective method of destruction employed that meet NISPOM standards?			

NISPOM language does not require prior approval for any of the listed methods of destruction

5-706	Is classified material destroyed by appropriately cleared contractor employees?			

The NISPOM requires two persons for the destruction of TOP SECRET and one person for the destruction of SECRET and CONFIDENTIAL.

5-707	Are proper records maintained for the destruction of TOP SECRET classified and do those who sign have actual knowledge of the material's destruction?			

The NISPOM has eliminated the accountability requirement for SECRET classified material. However, keep in mind the U.S. Government reserves the right to retrieve its classified material or cause appropriate disposition. Thus, your information management system shall be capable of facilitating such retrieval and disposition in a reasonable period of time. [5-201]

5-708	Is classified waste properly safeguarded until its timely destruction?			

Q. REPRODUCTION

NISPOM REF:	Question:	YES	NO	N/A
5-600	Is reproduction of classified material kept to a minimum?			

Effective access control through facility configuration, technology, and operational procedures is encouraged and should be published in the SPP.

5-600	Is the reproduction of classified accomplished only by properly cleared, authorized, and knowledgeable employees?			
5-601	Is reproduction authorization obtained as required?			
5-602	Are reproductions of classified material reviewed to ensure that the markings are proper and legible?			

Any review of a classified reproduction job should include concern for waste, trimmings, copy overruns, etc., and any materials used in production which may retain classified information or images requiring destruction or safeguarding.

5-603	Is a record of reproduction maintained for accountable material and is it retained as required?			

Remember, the NISPOM requires a formal accountability system for Top Secret material, and an Information Management System for Secret and Confidential material. [5-201; 5-203].

R. CLASSIFIED MEETINGS (sponsored by the Government)

NISPOM REF:	Question:	YES	NO	N/A
6-200 6-201	Is Government sponsorship requested for classified meetings as required?			
6-201b	Are classified meetings held at approved locations?			
6-201c	Has the contractor developed adequate security procedures, for the requested meeting, and submitted them to the authorizing agency for approval?			
6-201c (2)	Is attendance limited to persons appropriately cleared who have the need-to-know?			
6-201c (3) and 6-202	Is prior written authorization obtained, from the relevant Government Contracting Activity, before disclosure of classified information?			

Remember that classified presentations shall be delivered orally and/or visually. Copies of classified presentations, slides, etc. shall not be distributed at the meeting but rather safeguarded and transmitted as required in the NISPOM. [6-200; 5-400].

6-202b	Has a copy of the disclosure authorization been furnished to the Government agency sponsoring the meeting?			

Authority to disclose classified information at meetings, whether by industry or government, must be granted by the Government Contracting Activity having classification jurisdiction. [6-202]

6-203	Are contractor employees properly screened for clearance and need-to-know prior to attending a classified meeting?			

S. CONSULTANTS				
NISPOM REF:	**Question:**	**YES**	**NO**	**N/A**

For security administration purposes, the consultant shall be considered an employee of the hiring contractor or GCA. The using (hiring) contractor or GCA shall be the consumer of services offered by the consultant it sponsors for a personnel clearance. [2-213].

2-213	Has the consultant and the using contractor or GCA jointly executed a “consultant certificate” setting forth their respective security responsibilities?			
2-213	Does the consultant possess classified material at his/her place of business?			

T. INFORMATION SYSTEMS

System No.	**Overall Review Finding:**	**Reviewed By:**	**Date:**

Administrative				
NISPOM REF:	**Question:**	**YES**	**NO**	**N/A**
8-202.	Has written accreditation for the SSP been obtained from DSS?			
8-202a.	If no, was interim approval granted? Up to 180 Days □ 181 to 360 Days □			
8-202.	Did the user begin processing classified information before interim approval or written accreditation?			
8-202a.	If interim approval was granted, has the specified time period expired?			
8-202g.	Has the Information System Security Manager (ISSM) been authorized self-certification authority?			
8-202g.	If yes, does the ISSM certify all IS under the Master SSP?			
ISL 01L-1.	If yes, does the ISSM provide notification to DSS?			
8-202d.	Does the IS require reaccreditation based on 3 year limit?			
8-202e.	Has accreditation been withdrawn?			
8-202f.	Has accreditation been invalidated?			
8-202e.	If withdrawn or invalidated, has memory and media been sanitized?			
Responsibilities				
8-101b.	Has management published and promulgated an IS Security Policy?			
8-101b.	Has an ISSM been appointed?			
8-103.	If yes, are the ISSM's duties and responsibilities identified and being carried out?			
8-104.	Has the ISSM designated one or more Information System Security Officer(s) (ISSOs)?			
8-104.	If yes, are the ISSO(s) duties and responsibilities identified and being carried out?			
8-307.	Are the privileged users duties and responsibilities identified and understood?			
8-307.	Are the general users responsibilities identified and understood?			
System Security Plan (SSP)				
8-402.	What protection level (PL) is authorized? PL 1 □ PL 2 □ PL 3 □ PL 4 □			
8-401.	Highest level of data processed? Confidential □ Secret □ Top Secret □			
User Requirements				
Table 4.	Clearance level of privileged users Confidential □ Secret □ Top Secret □			
Table 4.	Clearance level of general users Confidential □ Secret □ Top Secret □			
Table 4.	Do the users understand the need-to-know requirements of the authorized PL?			
8-303a.	How is the user granted access to the IS? User-IDs □ Personal identification □ Biometrics □			
ISL 01L-1.	If passwords are used, does the user understand his/her responsibility for password creation deletion, changing, and length?			
8-311.	Is the "user" involved in configuration management (i.e., adding/changing hardware, software, etc)?			
8-311.	If yes, does the user understand and following the configuration management plan?			

IS Hardware				
NISPOM REF:	**Question:**	**YES**	**NO**	**N/A**
8-311a.	Does the SSP reflect the current hardware configuration?			
8-311d.	If not, does the maintenance logs reflect changes in the hardware configuration?			
8-306a.	Does the IS equipment bear appropriate classification markings?			
Physical Security				
8-308.	How is the IS physically protected? (Check all that apply) Closed Area □ IS Defined Perimeter Boundary Area (Restricted Area) □ Approved Containers □ PDS [1] □ Approved Locks □ Access Control Devices □ Alarms □ Guards □ Patrols □ Seals □ Other (Specify) □ [1] Protected Distribution System Intrusion Detection System □			
5-800.	If closed area, are all construction requirements met?			
5-306.	Is access controlled by cleared employee, guard or supplanting access control device?			
5-306.	If access is controlled by cleared employee, what criteria is used before granting access?			
5-312.	If access is controlled by a supplanting access control device, are all requirements met?			
5-307.	If required, is supplemental protection provided by guards or an approved IDS?			
5-307b.	If supplemental protection is provided by guards, are all requirements met?			
5-900.	If supplemental protection is provided by an IDS, are all requirements met?			
5-306a.	Is open shelf or bin storage of classified information, media or equipment approved?			
NSTISSI 7003.	If classified wirelines leave the closed area, are all PDS construction requirements met?			
NSTISSI 7003.	If PDS is used, are all inspection requirements followed?			
NSTISSI 7003.	If PDS is used, do they contain unclassified wirelines?			
	If closed area has false ceilings or floors, are transmission lines not in a PDS inspected at least: Monthly (Security In-Depth) □ Weekly (No Security In-Depth) □			
8-502b.	If restricted or IS protected area, is the IS downgraded before/after use?			
ISL 01L-1.	If seals are used to detect unauthorized modification, are the website guidelines followed?			
ISL 01L-1.	If seals are used, does the audit log reflect why the seal was replaced?			
8-308c.	Is visual access to the IS or classified information obtainable by unauthorized individuals?			
Software				
ISL 01L-1.	Are contractor personnel that handle system or security related software appropriately cleared?			
8-302a.	Are the installation procedures identified in the SSP being followed?			
8-306c.	Is the media on which software resides write-protected and marked as unclassified?			
8-306c.	Is non-changeable media (e.g. CD read-only) appropriately handled and marked?			
8-202c.	Is security relevant software evaluated before use?			
8-305.	Is software from an unknown or suspect origin used?			

8-305.	If used, how is the software validated before use?			
Software				
NISPOM REF:	**Question:**	**YES**	**NO**	**N/A**
8-305.	Is software tested for malicious code and viruses before use?			
8-305.	Are incidents involving malicious software handled in accordance with SSP procedures?			
8-502d.	Is separate media maintained for periods processing?			
Media				
8-306.	Is media marked to the classification level of the data?			
5-300.	Is media appropriately safeguarded when not in use?			
ISL 01L-1.	Are approved procedures followed when unclassified media is introduced into the system?			
Security Audits				
ISL 01L-1.	Are all appropriate Audit entries recorded?			
8-602a.	Are processing times reasonable (i.e., hours between breaks)?			
8-602.	Are the protection requirements for each audit requirement recorded?			
8-602a.	Are the Audit Logs/Records reviewed weekly □ Daily □			
8-602a.	Is the reviewer authorized and briefed on what and how to review the audit records?			
8-602.	Does the reviewer understand his/her responsibility for handling audit discrepancies?			
8-602/ISL 01L-1.	Are audit Logs/Records retained for 12 months?			
Security Awareness				
8-103a.	Has the contractor implemented an IS training program?			
8-103a.	Are users briefed before access is granted?			
IS Operations				
8-502.	If possible, have the user step through the security level upgrading procedures.			
8-502.	Is the user responsible for clearing memory and buffer storage?			
8-502.	If yes, does the user know how to clear memory and buffer storage?			
8-502.	Is magnetic media cleared/sanitized before and after classified processing?			
8-310.	Does the user understand his/her responsibility for handling/reviewing data and output (in-use controls)?			
8-310/ISL 01L-1.	Does the user follow approved procedures when doing a trusted download?			
8-310/ISL 01L-1.	If possible, have the user step through the security level downgrading procedures.			
Maintenance and Repair				
8-304a.	Is maintenance done at the contractor's facility with cleared personnel?			
8-304a.	If yes, is need-to-know enforced?			
8-304b.	Is maintenance done at the contractor's facility with uncleared personnel?			
8-304b.	If yes: are the maintenance personnel U.S. citizens?			

8-304b	Does the escort understand his/her responsibilities?			

Maintenance and Repair

NISPOM REF:	Question:	YES	NO	N/A
ISL 01L-1.	Does the audit log reflect the escorts name?			
ISL 01L-1.	Is diagnostic or maintenance done from a remote location using secured/nonsecured comm. lines?			
ISL 01L-1.	Is maintenance physically done away from the contractor's facility?			
8-304b (4)	If uncleared maintenance personnel, is a dedicated copy of the operating system software maintained?			
8-304b.	Is the system and diagnostic software protected?			
8-304b.	Is the entire IS or individual components sanitized before/after maintenance?			
8-103.	Has the ISSM approved the use of maintenance tools and diagnostic equipment?			
	Media Cleaning, Sanitization and Destruction			
8-502.	Is the user responsible for clearing memory (volatile/nonvolatile)?			
8-502.	Is the user responsible for sanitizing memory (volatile/nonvolatile)?			
ISL 01L-1.	If yes, does the user annotate the audit records?			
8-502.	Ask the user to describe or step through the procedure.			
8-502.	Is the user responsible for clearing magnetic storage media?			
8-502.	Is the user responsible for sanitizing magnetic storage media?			
ISL 01L-1.	If yes, does the user annotate the audit records?			
8-502.	Ask the user to describe or step through the procedure?			
ISL 01L-1.	Is an approved overwrite utility used to clear or sanitize magnetic media?			
ISL 01L-1.	If yes, does the user annotate the audit records?			
IA Website.	Does the contractor have approved procedures for the destruction of non-magnetic media (e.g. Optical Disks)?			
ISL 01L-1.	What level magnetic tape is used? Type I □ Type II □ Type III □ Unknown □			
ISL 01L-1.	Does the contractor use an approved tape degausser to sanitize magnetic tapes?			
	If yes, what level tape degausser? Type I □ Type II □ Type III □ Unknown □			
	If yes, does the user annotate the audit records?			
	If yes, is the tape degausser within NSA specifications?			
ISL 01L-1.	Are approved procedures followed for clearing/sanitizing Printers?			
	STU-III			
	Is a STU-III used for classified data transmission?			
	If yes, are users briefed on proper use and security practices?			
	Are installed terminals supported by a COMSEC account or hand carry receipt?			
	Are installed terminals in controlled areas?			
	Does the SSP reflect the outside STU-III connections?			
	If yes, has someone verified the outside connections are authorized and accredited?			

Networks				
NISPOM REF:	**Question:**	**YES**	**NO**	**N/A**
8-700.	Are all outside network connections known, authorized and accredited?			
8-700e(3).	If the network leaves the contractor's facility, are NSA approved encryption device(s) used?			
8-700b.	Is this a unified network?			
8-700c.	Is this an interconnected network?			
8-700c.	If yes: does each participating system or network have an ISSO?			
8-700c.	Does the network have a controlled interface?			
8-610a.	Is the contractor following a network security plan?			
8-700.	Is this a contractor only network?			
8-700.	If no, is a DISN circuit being used or has the customer obtained a waiver from DISA?			
	If the network is not contractor only, has a MOU been coordinated between all DAAs?			
ISL 00L-1.	Are data transfers (receipt and dispatch) across the network audited?			

U. COMSEC/ CRYPTO

The primary source of information for COMSEC inspections is the NSA Industrial COMSEC Manual (NSA Manual 90-1). The NISPOM does not provide detailed guidance for protection of COMSEC material.

The following recommended checklists may be used to review a “Traditional COMSEC Account” (pages 21-25), or a ”Seed Key Only COMSEC Account” (SOCA) (pages 26-28).

TRADITIONAL COMSEC ACCOUNT

(Pages 21-25)

ORGANIZATION:

COMSEC Account Number:

Date:

SCOPE OF THE VISIT				
Reference:	**Question:**	**YES**	**NO**	**N/A**
NSA Ind. COMSEC Man. 90-1, Para 38.a	Does account have a complete and accurate Register file?			
COMMENTS:				
NSA Ind. COMSEC Manual 90-1, Para. 37.d (1)(e); Para 38.a. (1)-(2).	Is the COMSEC register file contained in DIAS?			
COMMENTS:				
NSA Ind. COMSEC Manual 90-1, Para. 37.d (1)(e); Para 38.a. (1)-(2).	Does the COMSEC Register File consist of:	**L6061's**	**DIAS**	**Company Design**
COMMENTS: NOTE: Use of any Company Design has to have prior approval of Y131.				
NSA Ind. COMSEC Man. 90-1, Para 42.a.(3); Para 42.a.(5).	Have all transactions reflecting corrections to the COR's inventory been acquired?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 123.	Have all follow-up actions identified during a previous audit been completed?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 37.d.	Are all COMSEC accounting files complete and accurate?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 11.a.(1); Para 17.a.(1); Para 17.b.(1)	Are the number of personnel currently managing the account sufficient and granted all necessary access?			
COMMENTS:				
NSA Man. 90-1 (NICM), Para 17.a.(3)	Have current DD Form 254s, MOUs, or MOAs, as applicable, been reviewed for compliance with security requirements?			
COMMENTS:				

SCOPE OF THE VISIT

Reference:	**Question:**	**YES**	**NO**	**N/A**
NSA Ind. COMSEC Man. 90-1, Para 50.a; **NSTISSI No. 4005, Sec. VIII, Para. 36.**	Is access to COMSEC containers storing future editions of Operational Key restricted to account personnel (Custodian.Alternate(s)/FSO)?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 39.b.(2); Para 39.b.(4); Para 39.c.; NSTISSI No. 4005, Sections IX, Para 48.i.; Para 48.j.	Do hand receipts reflect current holder(s)?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 37.c. Para 39.c.; Para 39.e.	Are hand receipts for remote holders updated every six months?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 17.c.(5); Section XII, Para 91-93.	Are combinations (where required) properly recorded, marked, nomenclated in the document control system, and issued to the FSO for storage?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 91.c. (1)-(5); NSTISSI No. 4005, Section XV, Para 98.	Are combinations changed at least every two years or as needed (event driven) for all containers holding COMSEC accountable material?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 1.c.; Para 17.c.(1); Para 39.b.(3)	Have COMSEC Standard Operating Procedures (SOP) been developed?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 17.a.(20); Section XV, Para 102-110.	Has an Emergency Action Plan been incorporated in the SOP?			
COMMENTS:				

SCOPE OF THE VISIT				
Reference:	**Question:**	**YES**	**NO**	**N/A**
NSA Ind. COMSEC Man. 90-1, Para 77; Secion IX, Para 66-77.	Have written STU-III education procedures/briefings been developed, and issued to the appropriate individuals?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 37.d.(2)(b).	Are INFOSEC Bulletins being received by the custodian regularly and maintained?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 17.a. (12).	Does the account hold Operational, On-The-Air-Test, Maintenance, or SEED Key?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 17.a.(14); Para 17.a.(15); NSTISSI No. 4005, Section XIII, Para 69.	Is a Protective Technologies Program in place for inspecting incoming shipments of COMSEC material?			
COMMENTS:				
NSA Ind. COMSEC Manual 90-1, Para 39.d; Para 49.d; Para 50.b (2); Para 86; Para 87.a.(1) Para 88.c(1); Para 89.b.(1); NSTISSI No. 4005, Section IX, Para 42.a.; Section XI, Para 64.c.; Section XIII, Para 72.	Two Person Integrity (TPI)?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 98; para 117; NSTISSI No. 4003, ANNEX C (Practices Dangerous to Security – PDS).	Is the account holding superseded Seed Key or manuals?			
COMMENTS:				

SCOPE OF THE VISIT				
Reference:	**Question:**	**YES**	**NO**	**N/A**
NSA Ind. COMSEC Man. 90-1, Para 42.a.(4); (SEE-INFOSEC BULLETIN No. 1-98, pg-6&7 FOR DISPOSITION OF CCI)	Is the account holding any excess COMSEC material?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 17.a.(11); **Para 45; Para 49.i.;**	Are all accountable manuals up to date; i.e., amendments posted (residue destroyed and a destruction report submitted to Y131), page checks performed, signature and amendment page(s) completed?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 49.h.;	(FOR CONTRACTORS ONLY) Are accountable COMSEC documents marked “COMSEC Material – Access By Contractor Personnel Restricted to U.S. Citizens Holding Final Government Clearance”?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 9; Para 39.	Do users/hand receipt holders know their responsibilities, and have they received a COMSEC Briefing?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 17a.(1), Para 17a.(4); Para 17.a. (12)-(16); NOTE: COMSEC INCIDENTS MUST BE REPORTED IAW the NSA Industrial COMSEC Manual 90-1, Para 114, to NSA I413, (410) 854-6811 (STU III capable)	Are all COMSEC accountable equipment, Keying material and manuals properly controlled and marked?			
COMMENTS:				
NTISSI No. 3013, Annex A, Para c.(2) (Phones not REKEYED – PDS); NSA Ind. COMSEC Man. 90-1, Para 73; Para 77; EKMS 702.01, Para 8.7.	STU-III:			
	Rekeyed at least annually?			
	Master CIK(s) properly stored?			
	User CIK(s) properly controlled & stored?			
	User(s) received Education Briefing?			
COMMENTS:				

<table>
<tr><th colspan="5">SCOPE OF THE VISIT</th></tr>
<tr><th>Reference:</th><th>Question:</th><th>YES</th><th>NO</th><th>N/A</th></tr>
<tr><td><b>Contact the NSA Y131 Training Office, on (301) 688-8110 ASAP to obtain the IAEC-211 prerequisite disk and register for the IAEC-2112 course.</b></td><td>Have the COMSEC Custodian and Alternate attended the mandatory COMSEC Custodian Training Course (IAEC-2112 – formerly ND-112)?</td><td></td><td></td><td></td></tr>
<tr><td colspan="5"><b>COMMENTS: Note: Recently appointed COMSEC Custodians and Alternate(s) must complete IAEC-2111/ND-111 (which is a prerequisite to IAE C-2112) prior to attending the course.</b></td></tr>
<tr><td colspan="5"><b>ADDITIONAL COMMENTS:</b></td></tr>
</table>

SEED ONLY COMSEC ACCOUNT
(SOCA)

(Pages 26-28)

ORGANIZATION:

COMSEC Account Number:

Date:

SCOPE OF THE VISIT				
Reference:	**Question:**	**YES**	**NO**	**N/A**
NSA Ind. COMSEC Man. 90-1, Para 38.a	Does account have a complete and accurate Register file?			
COMMENTS:				
NSA Ind. COMSEC Manual 90-1, Para. 37.d (1)(e); Para 38.a. (1)-(2).	Does the COMSEC Register File consist of:	**L6061's**	**DIAS**	**Company Design**
COMMENTS: Note: Use of any Company Design has to have prior approval of Y131.				
NSA Ind. COMSEC Man. 90-1, Para 42.a.(3); Para 42.a.(5).	Have all transactions reflecting corrections to the COR's inventory been acquired?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 123.	Have all follow-up actions identified during a previous audit been completed?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 37.d.	Are all COMSEC accounting files complete and accurate?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 11.a.(1); Para 17.a.(1); Para 17.b.(1)	Are the number of personnel currently managing the account sufficient and granted all necessary access?			
COMMENTS:				
NSA Man. 90-1 (NICM), Para 17.a.(3)	Have current DD Form 254s, MOUs, or MOAs, as applicable, been reviewed for compliance with security requirements?			
COMMENTS:				

SCOPE OF THE VISIT				
Reference:	**Question:**	**YES**	**NO**	**N/A**
NSA Ind. COMSEC Man. 90-1, Para 39.b.(2); Para 39.b.(4); Para 39.c.; NSTISSI No. 4005, Sections IX, Para 48.i.; Para 48.j.	Do hand receipts reflect current holder(s)?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 37.c. Para 39.c.; Para 39.e.	Are hand receipts for remote holders updated every six months?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 17.c.(5); Section XII, Para 91-93.	Are combinations (where required) properly recorded, marked, nomenclated in the document control system, and issued to the FSO for storage?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 91.c. (1)-(5); NSTISSI No. 4005, Section XV, Para 98.	Are combinations changed at least every two years or as needed (event driven) for all containers holding COMSEC material?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 1.c.; Para 17.c.(1); Para 39.b.(3)	Have COMSEC Standard Operating Procedures (SOP) been developed?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 17.a.(20); Section XV, Para 102-110.	Has an Emergency Action Plan been incorporated in the SOP?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 77; Secion IX, Para 66-77.	Have written STU-III education procedures/briefings been developed, and issued to the appropriate individuals?			
COMMENTS:				

SCOPE OF THE VISIT				
Reference:	**Question:**	**YES**	**NO**	**N/A**
NSA Ind. COMSEC Man. 90-1, Para 37.d.(2)(b).	Are INFOSEC Bulletins being received by the custodian regularly and maintained?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 17.a.(14); Para 17.a.(15); NSTISSI No. 4005, Section XIII, Para 69.	Is a Protective Technologies Program in place for inspecting incoming shipments of COMSEC material?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 98; para 117; NSTISSI No. 4003, ANNEX C (Practices Dangerous to Security – PDS).	Is the account holding superseded Seed Key?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 42.a.(4); (SEE-INFOSEC BULLETIN No. 1-98, pg-6&7 FOR DISPOSITION OF CCI)	Is the account holding any excess COMSEC material?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 9; Para 39.	Do users/hand receipt holders know their responsibilities, and have the FSO/Custodian/Alternate and User Rep received a COMSEC Briefing?			
COMMENTS:				
NSA Ind. COMSEC Man. 90-1, Para 17a.(1), Para 17a.(4); Para 17.a. (12)-(16);	Is all COMSEC accountable equipment and Keying material properly controlled and marked?			
COMMENTS: NOTE: COMSEC INCIDENTS MUST BE REPORTED IAW the NSA Industrial COMSEC Manual 90-1, Para 114, to NSA I413, (410) 854-6811 (STU III capable)				
NTISSI No. 3013, Annex A, Para c.(2) (Phones not REKEYED – PDS); NSA Ind. COMSEC Man. 90-1, Para 73; Para 77; EKMS 702.01, Para 8.7.	STU-III:			
	Rekeyed at least annually?			
	Master CIK(s) properly stored?			
	User CIK(s) properly controlled & stored?			
	User(s) received Education Briefing?			
COMMENTS:				

V. INTERNATIONAL OPERATIONS				
NISPOM REF:	**Question:**	**YES**	**NO**	**N/A**
	Disclosure of U.S. Information to Foreign Interests			
If YES **Continue!**	Does the contractor have any classified contracts with foreign interests?			
10-200 **10-202**	Was an export license or a written letter of authorization obtained prior to disclosure of classified information?			

Remember that an export authorization is required before the contractor makes a proposal to a foreign person that involves eventual disclosure of U.S. classified information. [10-202]

10-201	Is proper disclosure guidance provided by the Government Contracting Activity?			
10-203	Are requests for export authorizations of significant military equipment or classified material accompanied by Department of State, Form DSP-83, Non-Transfer and Use Certificate?			
10-204	Have the required security clauses and classification guidance been incorporated into the subcontract document for all direct commercial arrangements with foreign contractors involving classified information?			

For examples of security requirement clauses see page 10-2-3, NISPOM.

	Possession of Foreign Classified Information			
NISPOM REF:	**Question:**	**YES**	**NO**	**N/A**
10-301	Has the DSS been notified of all contracts, awarded by foreign governments, that involve access to classified information?			
10-300	Is foreign government information provided protection equivalent to that required by the originator?			

Foreign government classified generally parallels our three-level system. However, occasionally you will see the marking "RESTRICTED." ISL 95L-2, ISL 96L-1, and ISL 03L-1 provide guidance on the handling of "Restricted" information.

10-303	Are U.S. documents containing foreign government classified information marked as required by the NISPOM?			
10-305	Are contractor employees, handling foreign classified information, briefed prior to access and is it acknowledged in writing?			
10-306	Is foreign government material stored in a manner that prevents its mingling with other material?			
10-309	Is transfer of foreign government information outside the U.S. handled on a government-to-government basis?			

The receipt of classified material from a foreign source through non-government channels shall be promptly reported to the DSS Field Office. [10-316]

10-312	Is the subcontracting of contracts involving access to foreign government information conducted in accordance with the NISPOM?			

	International Transfers			
NISPOM REF:	**Question:**	**YES**	**NO**	**N/A**
10-401	Do all international transfers of classified material take place through government-to-government channels?			
10-401 **10-402**	Is an appropriate transportation plan prepared for each contract involving international transfer of classified material via freight forwarder or commercial carrier?			
10-405	Does the use of freight forwarders for the transfer of classified material meet the requirements of the NISPOM?			
10-406	Is classified material handcarried outside of the U.S.? If so, is such action always approved by the DSS?			
10-406 b-c	Are couriers provided with a Courier Certificate and do they execute a Courier Declaration before departure?			

Paragraphs (10-406a thru j) provide detailed requirements for employees acting as couriers when handcarrying classified across international boundaries.

10-407	Are all international transfers of classified controlled by a system of continuous receipts?			
10-408, **10-409**	Is adequate preparation and documentation provided for international transfer of classified pursuant to commercial/GCA sales or ITAR exemption?			

	International Visits and Control of Foreign Nationals			
NISPOM REF:	**Question:**	**YES**	**NO**	**N/A**
10-501 **10-506** **10-507**	Has the contractor established procedures to monitor/control international visits by their employees and by foreign nationals?			

Visit authorizations shall not be used to employ the services of foreign nationals to access export controlled materials; an export authorization is required in such situations. [10-501c]

10-506	Are requests for visits abroad by U.S. contractors submitted on a timely basis?			

The Visit Request format is contained on pages 10-5-4 and 10-5-5.

10-508 **10-509**	Does the contractor properly control access to classified by on-site foreign nationals?			

All violations of administrative security procedures or export control regulations by foreigners shall be reported to the CSA. [10-510].

	Contractor Operations Abroad			
NISPOM REF:	**Question:**	**YES**	**NO**	**N/A**

The storage, custody, and control of classified information required by U.S. contractor employees abroad is the responsibility of the U.S. Government.

10-604	Are employees assigned abroad properly briefed on the security requirements of their assignment?			
10-605a.	Is the CSA advised of cleared employees assigned abroad for periods exceeding 90 days?			
10-603	Has all transmission of classified information to cleared employees overseas been conducted through U.S. Government channels?			

(ISL 96L-2) ***Consultants are eligible for access to classified information outside the U.S., provided overseas travel does not exceed 90 consecutive days.***

	NATO Information Security Requirements			
NISPOM REF:	**Question:**	**YES**	**NO**	**N/A**
10-705	Are briefings/debriefings of employees accessing NATO classified conducted in accordance with the NISPOM, and are the appropriate certificates and records on file?			

Remember that a personnel clearance is not required for access to NATO RESTRICTED, although a Facility Security Clearance is required. (NISPOM 10-703 & 10-704).

10-708	Are all classified documents properly marked?			
10-709	Has the contractor received adequate classification guidance?			
10-711	Have the combinations to containers holding NATO classified been changed annually as a minimum?			
10-712	Has all NATO classified been properly received and transmitted?			
10-716	Are the accountability records for NATO classified maintained as required?			
10-720	Are visits of persons representing NATO properly handled and is the visit record maintained as required?			

W. OPSEC				
NISPOM REF:	**Question:**	**YES**	**NO**	**N/A**
None	Are OPSEC requirements implemented in accordance with contractual documentation provided by the GCA?			

X. SPECIAL ACCESS PROGRAMS (SAP)

Reference:	Question:	Yes	No
NISPOM, NISPOM Supplement, and DoD Overprint to the NISPOM Supplement	Does the facility have any Special Access Program contract activity? Note: The FSO should discuss this with the senior management official of the facility.		
	If Yes: Remember that such programs are subject to NISPOM, NISPOM Supplement, DoD Overprint to the NISPOM Supplement and Program Security Guide requirements.		
	If Yes: During the self-inspection it is important for the FSO to coordinate with the internal Contractor Program Security Officer (CPSO) to ensure that individual program security requirements are being followed.		

Suggested Questions When Interviewing Uncleared Employees:

- □ What is classified information?
- □ Have you ever seen classified information?
- □ If you found classified information unprotected, what would you do?
- □ Have you ever heard classified information being discussed?
- □ Have you ever come into possession of classified materials? How?

Suggested Questions When Interviewing Cleared Employees:

- □ What is your job title/responsibility?
- □ Which contract or program requires the use of your clearance? How?
- □ What is the level of your security clearance?
- □ How long have you been cleared?
- □ When was your last access to classified information and at what level?
- □ Have you ever accessed classified information outside of this facility?
- □ Did anyone else from the facility accompany you on this visit?
- □ What procedures did you follow prior to your classified visit?
- □ Did you take any classified notes or classified information back to the facility?
- □ What procedures were followed to protect this information?
- □ Where is this information now?
- □ Have you ever allowed visitors to have access to classified information?
- □ How did you determine their need-to-know?
- □ Have you ever been approached by anyone requesting classified information?
- □ Do you ever work overtime and access classified information?
- □ When was the last time that you had a security briefing?
- □ What can you recall from this briefing?

□ Can you recall any of the following being addressed in briefings?

- Risk Management
- Public Release
- Adverse Information
- Job Specific Security Brief
- Safeguarding Responsibilities
- Counterintelligence Awareness

□ What is meant by the term adverse information and how would you report it?

□ Can you recall any other reportable items?

□ Have you ever been cited for a security violation?

□ What would you do if you committed a security violation or discovered one?

□ Do you have the combination to any storage containers, Closed Areas, etc.?

□ Who other than yourself has access to these containers?

□ Is a record maintained of the safe combination? If so, where?

□ Do you reproduce or generate classified? If so, what controls are established?

□ Where do you typically work when you generate classified information?

□ What procedures do you follow to protect classified while working on it?

□ Do you ever use a computer to generate classified information?

□ How do you mark this information?

□ Please produce the classification guidance that you used. Is it accurate?

□ Are you aware of the procedures for challenging classification guidance?

□ What are the security procedures for publishing classified papers, etc.?

□ What procedures do you employ when handcarrying classified material?

□ Have you ever reproduced classified information? Describe the procedures.

□ Have you ever destroyed classified information? What procedures were used?

□ Do you have any questions regarding security?

Note: In addition to asking questions, it is a good idea to ask cleared employees to demonstrate how they perform their security-related tasks. (i.e. "Show me how you begin when you work with classified information on your computer?" Or; "Show me how you prepare a package for shipment?" This will allow you to see if classified information is being protected.

The Program Specific Self-Inspection Process

Both correspondence courses, *Essentials of Industrial Security Management* and *Protecting Secret and Confidential Documents,* identified the security concerns addressed during the self-inspections of non-possessing and possessing facilities. The scenarios described for you the self-inspection efforts of Harold Huxtable, FSO at the Electric Widget Company (EWC). Because EWC is a small facility which performs on one classified contract, any self-inspection effort would be, by default, a program specific inspection.

Are there any benefits to using the program specific approach when conducting the self-inspection of a larger facility with substantial classified involvement on a variety of programs? The program specific self-inspection can help you gain a better understanding of what your company's responsibility is for a particular classified program in addition to providing you insight as to what each person contributes to the effort. The following is provided to explain the program specific self-inspection.

Your DSS Office puts great emphasis on providing recommendations and suggestions to *improve* your security practices. But this can only be accomplished when you have a good grasp of your operations and the manner in which classified information is handled. By taking a detailed look at one or more classified programs and interviewing key individuals to determine what they do and how they handle classified information, you will be able to evaluate how well your facility's *overall* security program is functioning. Many classified programs require a variety of taskings such as manufacturing, report writing, testing, receipt, and transmission, etc. In a program specific inspection, you select one or more programs to be closely examined. This process usually begins with the interview of the program manager (in some facilities this could even be the President) to learn what the program or contract is all about.

Start by asking for a layman's overview of the program, and question the level of classified access required, the procedures for classifying information, what, if any, problems have been experienced, and who in the facility is responsible for what on the program. This leads to interviews with other employees including technical, clerical, and secretarial personnel. During these interviews, you should explore all security requirements connected with the employee's responsibility in the program such as classified material controls, classified storage, markings, classification management, transmission, disposition, security education, and reproduction. Elements of a more administrative nature, relating to the facility's security program, such as the review of visit authorization letters and briefing statements, are ordinarily covered by reviewing your records within the Security Office. *The main rule is: if the element is applicable to your facility's classified involvement, cover the element in your self-inspection and, whenever possible, consider using the program specific techniques illustrated below.*

You may find that exploring one classified program is not enough to give you a "feel" for how well your security program is functioning. One program may represent only a small part of the classified activity that takes place at your facility. If that's the case, you will want to examine several, if not all, of your classified programs in detail. It's important that you explore each inspection element thoroughly to ensure that your facility is in compliance with the NISPOM. Your underlying concern is that classified information and materials are properly protected and that your employees are knowledgeable of their security responsibilities.

A Program Specific Self-Inspection Scenario

The following scenario illustrates a self-inspection conducted on a specific program. For the purpose of this example, it is not an all-inclusive inspection.

Fenster Dinwiddie, FSO of Capabilities Limited (CL) has decided to focus his self-inspection on the SCUD Intercept Countermeasure (SIC) Project, one of three classified contracts awarded to CL. As we join Fenster, he has accomplished most of the administrative portion of the inspection. He has reviewed Letters of Consent, Briefing Statements, Personnel Security Clearance Change Notifications, etc., and has completed his inventory of all classified materials and records. He has already touched base with the President of CL to make sure there were no recent organizational changes or foreign involvement that he should report. Certain elements like Subcontracting, Consulting, COMSEC, and International Operations do not apply.

Emulating the inspection techniques formerly used by his IS Rep, Fenster has decided to go out on the floor and find out what the employees do and how knowledgeable they are about their security responsibilities.

The Program Manager Interview

Fenster recalled that his IS Rep began each inspection by interviewing the person most knowledgeable about a particular contract. In this case it means talking to Conrad Floot, the lead engineer on the SIC Project.

Fenster went upstairs to "Engineering Row" to locate Conrad. "Fenster!" cheered the engineers as he entered the department. Fenster is always tickled to receive such a salutation. He feels honored to maintain such a congenial relationship with the engineers. After all, he does represent the security department.

"Say, Conrad, can you fill me in on this SIC Project of yours? I'm doing my recurring self-inspection and decided to focus in on your program." Conrad is impressed. No one has ever expressed that much interest in his project before. And he loves to talk, especially about the SIC Project, his "baby" as he prefers to call it. "Sure, what do you need to know, Fence?"

"Well, why don't you start by giving me a program update. You know, what we're doing for the customer, what's classified about it, and things like that. But keep it simple, okay?" Conrad is thrilled. He proceeds to give Fenster a detailed overview of the program, its history, and current status. Fenster is thinking, "You know this is pretty interesting stuff. I should get out on the floor more often."

During the interview, Fenster took careful notes. He discovered that eight other engineers plus a contingent of secretarial and support personnel are working on at least some portion of the program. He decided he would interview each individual over the next couple of days. They discussed the classified design modifications which were being tested down the hall. Fenster had Conrad describe each step of the test procedure including whether aspects of the tests themselves were classified. He asked what makes the design modifications classified, how they're protected, who protects them, how and where they're tested, etc. To his relief, he found that all the procedures at least appeared to be in conformance with the NISPOM. Later, he would interview key members of the test and evaluation staff individually. He never realized there were so many security considerations!

Conrad identified his customer point-of-contact just in case Fenster or the IS Rep needed to call. They spent a lot of time on classification management. Fenster wanted to know what classification guidance had been provided by the customer and whether he felt that it was adequate. He asked what Conrad would do if they were to experience problems in determining what should be classified. They reviewed classified marking procedures, the kind of classified information that's been received, who is allowed access, procedures for generating classified information, reproduction, disposition, transmission, public release, and access authorizations. By the time he was done, Fenster had a pretty good idea of what the SIC Project was all about and whom to talk to for more information.

In addition to addressing the program-specific security concerns, Fenster remembered to question Conrad regarding important overall security program-related issues such as security education, adverse information, and foreign travel.

Employee Interviews

Next, Fenster interviewed each of the engineers on the project. He asked many of the same questions, but this time he was more interested in learning exactly what each person's responsibilities were and how they handled classified information. He already knew a great deal about the program just by talking to Conrad. It was time to "zero in" on the nuts and bolts of the SIC Project. His first stop was at Elmo Platz's office. According to Conrad, Elmo has been involved in the program from the start and, as the assistant program head, has major responsibilities.

First, Fenster asked Elmo to explain his job and how it relates to the SIC Project. Fenster asked what level of access he needed for the job, how he obtained his classification guidance and whether there were any problems in this area that he should be aware of.

There were other questions as well, all designed to determine whether Elmo and his SIC Project staff were following the requirements of the NISPOM. Fenster asked:

□ How often and under what circumstances did Elmo access classified information?

□ Was he aware of his adverse information reporting responsibilities?

□ Did he generate classified material in-house and, if so, on what equipment?

□ How was the information protected?

□ Did he have knowledge of the combination to the security container? Was the combination properly safeguarded?

□ Did he attend any classified meetings at the customer's site or at CL? Did anyone else from CL attend?

□ Did he reproduce classified material? On what equipment?

□ Was he familiar with the rules on retention, handcarrying, "need-to-know," marking, accountability, and disposition of classified information?

□ Was he aware of any unreported security violations?

□ Did any of his classified work require a special briefing, e.g., NATO?

□ Was there anything relating to security that he thought Fenster should know about?

□ Did he have any classified information that was not logged into the facility's accountability or Information Management System? Where did it come from?

You can see that Fenster was trying to cover all of the relative inspection elements listed in the self-inspection handbook during his interview. This line of questioning was continued with each of the major participants in the SIC Program, from the engineering staff to the mailroom personnel. When he was done, Fenster had covered every pertinent self-inspection element and had discovered only one or two administrative errors. His self-inspection was a success. We hope yours is, too!